

برمجة التطبيقات الاسلامكية

Lecture 2

By

Dr. Bhaa alhmdan

Hidden terminals problem

➤ Three mobile phones A, B, and C.

- ☐ The transmission range of A reaches B, but not C.
- ☐ The transmission range of C reaches B, but not A.
- ☐ The transmission range of B reaches A and C.
- ☐ A cannot detect C and vice versa.
- ☐ A starts sending to B, C does not receive this transmission.
- ☐ C also wants to send something to B and senses the medium.
 - ☐ The medium appears to be free for C.
 - ☐ C also starts sending causing a collision at B.
 - ☐ A cannot detect this collision at B and continues with its transmission.

Exposed node problems

- Hidden **terminals effect** only **causes** unnecessary delay.
 - B sends something to A and C wants to transmit data to some other mobile phone outside the interference ranges of A and B.
 - C senses the carrier and detects that the carrier is busy (B's signal).
 - C **postpones** its transmission until it detects the medium as being idle again.
 - But as A is outside the interference range of C, **waiting is not necessary**.
 - Causing a 'collision' at B does not matter because the collision is too weak to propagate to A. In this situation, **C is exposed to B**.

Infrastructure and ad-hoc networks

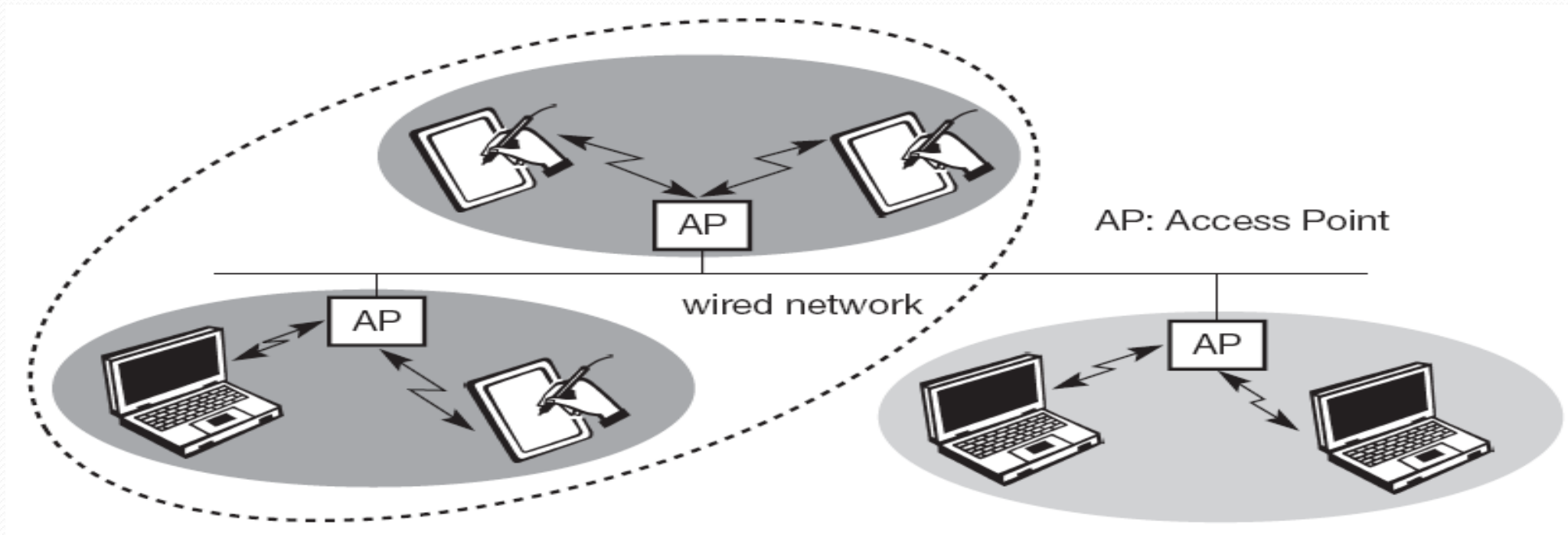
- Infrastructure networks provide access to other networks,

Include forwarding functions, medium access controletc.

- communication typically takes place only between the wireless nodes and the access point AP but not directly between the wireless nodes.
- The AP controls medium access, acts as a bridge to other wireless or wired networks.

Infrastructure and ad-hoc networks

- Several wireless networks may form one **logical wireless network**
 - APs together with the fixed network in between can connect several wireless networks to form a **larger network** beyond actual radio coverage.



Infrastructure and ad-hoc networks

- Collisions may occur if medium access of the wireless nodes and the access point is not coordinated.
 - If only the AP controls medium access, no collisions are possible.
- Typical cellular phone networks are infrastructure-based networks for a wide area.
- Also satellite-based cellular phones have an infrastructure – the satellites.
- Infrastructure does not necessarily imply a wired fixed network.

Infrastructure and ad-hoc networks

- Ad-hoc wireless networks do not need any infrastructure to work.
 - Each node can communicate directly with other nodes.
 - No AP controlling medium access is necessary.
- Nodes within an ad-hoc network can only communicate if they can reach each other physically.
 - if they are within each other's radio range or if other nodes can forward the message.
- In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms.
 - mechanisms to handle hidden or exposed terminal problems.

Infrastructure and ad-hoc networks

- Infrastructure-based and ad-hoc do not always come in their pure form.
 - Some networks rely on APs and infrastructure for basic services, but also allow for direct communication between the wireless nodes.
- Examples:
 - IEEE 802.11 and HiperLAN2 are typically infrastructure-based networks, which additionally support ad-hoc networking.
 - The Bluetooth, is a typical wireless ad-hoc network.

Wireless LAN

- WLAN is an access technology in **short-to-medium distances**, introduced first in **1999**.
 - WLANs gained importance especially in **home**, **office**, and campus environments.
 - **Low infrastructure cost**, **ease** of deployment and support for nomadic communication.
- **Problems:**
 - The **shared medium** (**performance degradation**) with the increasing number of stations (STAs).
 - **Maintaining Hight** (QoS) is difficult (link quality problems), **Security problems** : unauthorized access and eavesdropping in WLANs.

IEEE 802.11

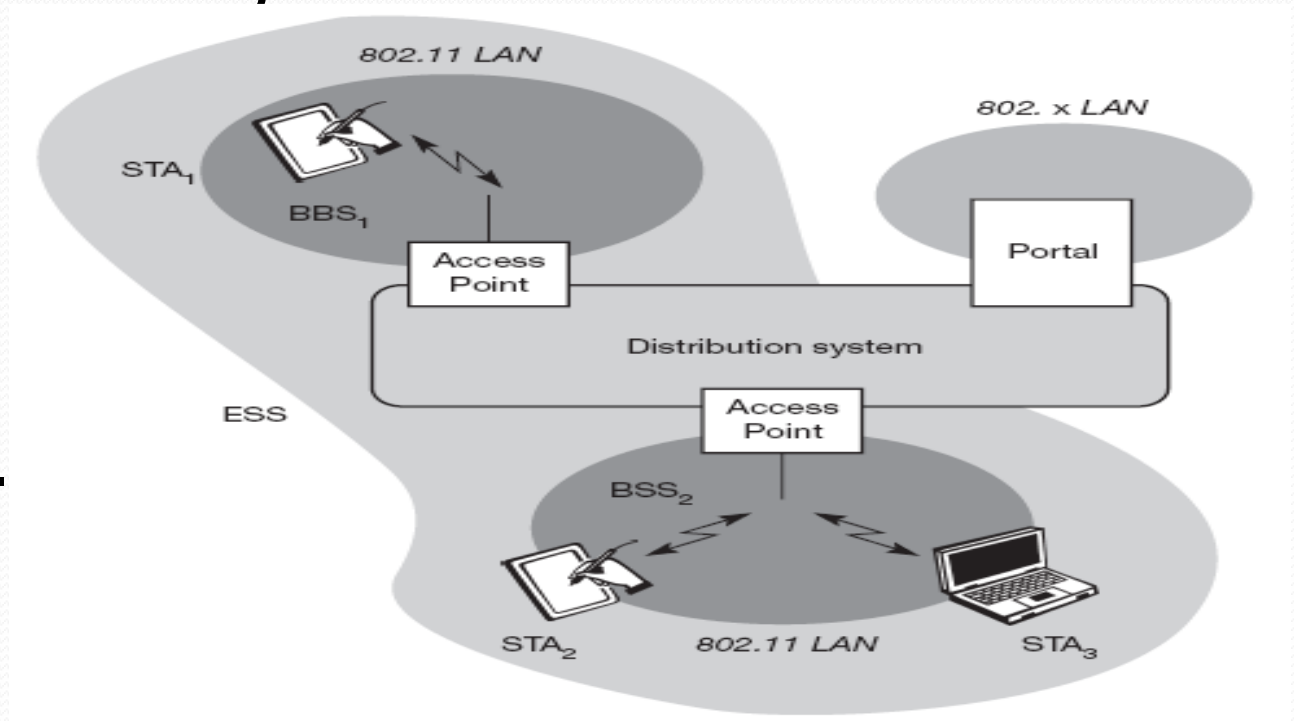
- IEEE standard 802.11 (IEEE, 1999).
 - It belongs to the **group of 802.x** LAN standards, e.g., **802.3** Ethernet or **802.5** Token Ring.
 - This means that the standard specifies the **physical and medium access layer adapted** to the special requirements of wireless LANs, **but offers** the **same interface as the others to higher layers** to maintain interoperability.
- 802.11 offers **time-bounded** and **asynchronous** services.
 - The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic.

IEEE 802.11: System architecture

- Nodes (stations) (STAi), are connected to Access Points (AP).
 - Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.
- The stations and the AP which are within the same radio coverage form a **Basic Service Set** (BSSi).
- A **Distribution System DS** connects several BSSs via the APs to form a single network and thereby **extends** the wireless coverage area.
 - This network is now called an **extended service set** (ESS) and has its own **identifier**, the **ESSID**.

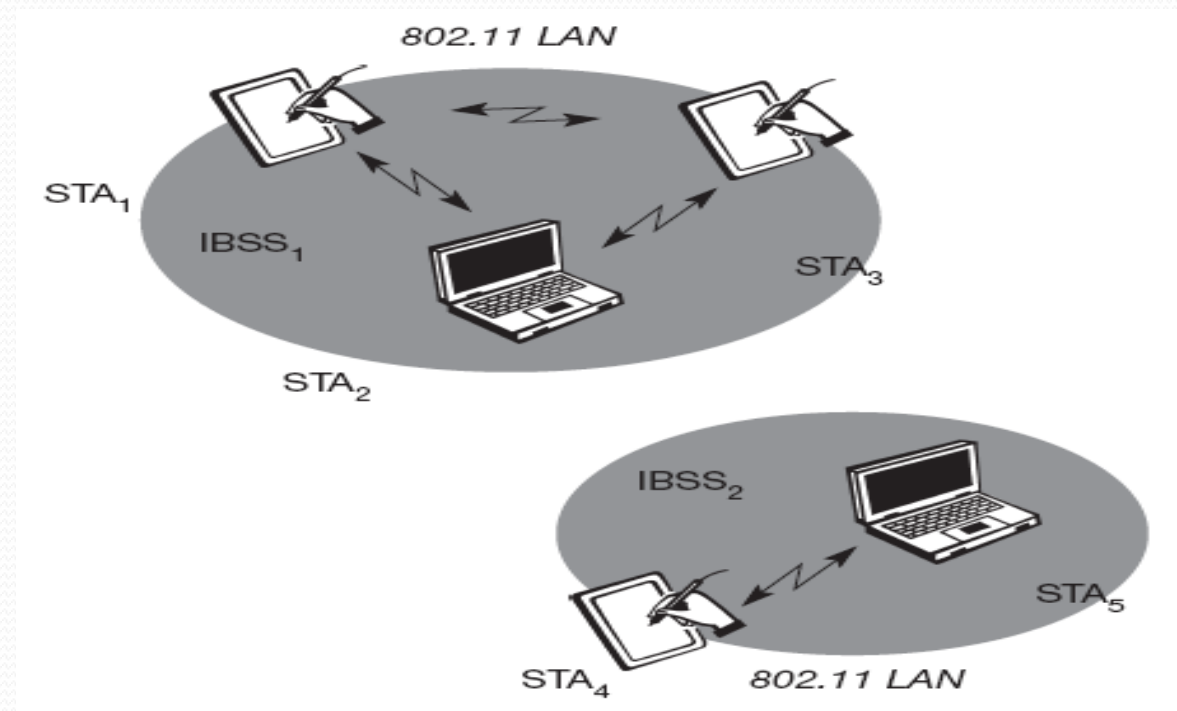
IEEE 802.11: System architecture

- The DS connects the wireless networks via the APs with a **portal**, which forms the interworking unit to other LANs.
- The DS could consist of bridged IEEE LANs, wireless links, or any other networks.
- **Need** for the additional standard IEEE 802.11f to specify an **inter access point** protocol.
 - can control medium access to support time-bounded service.



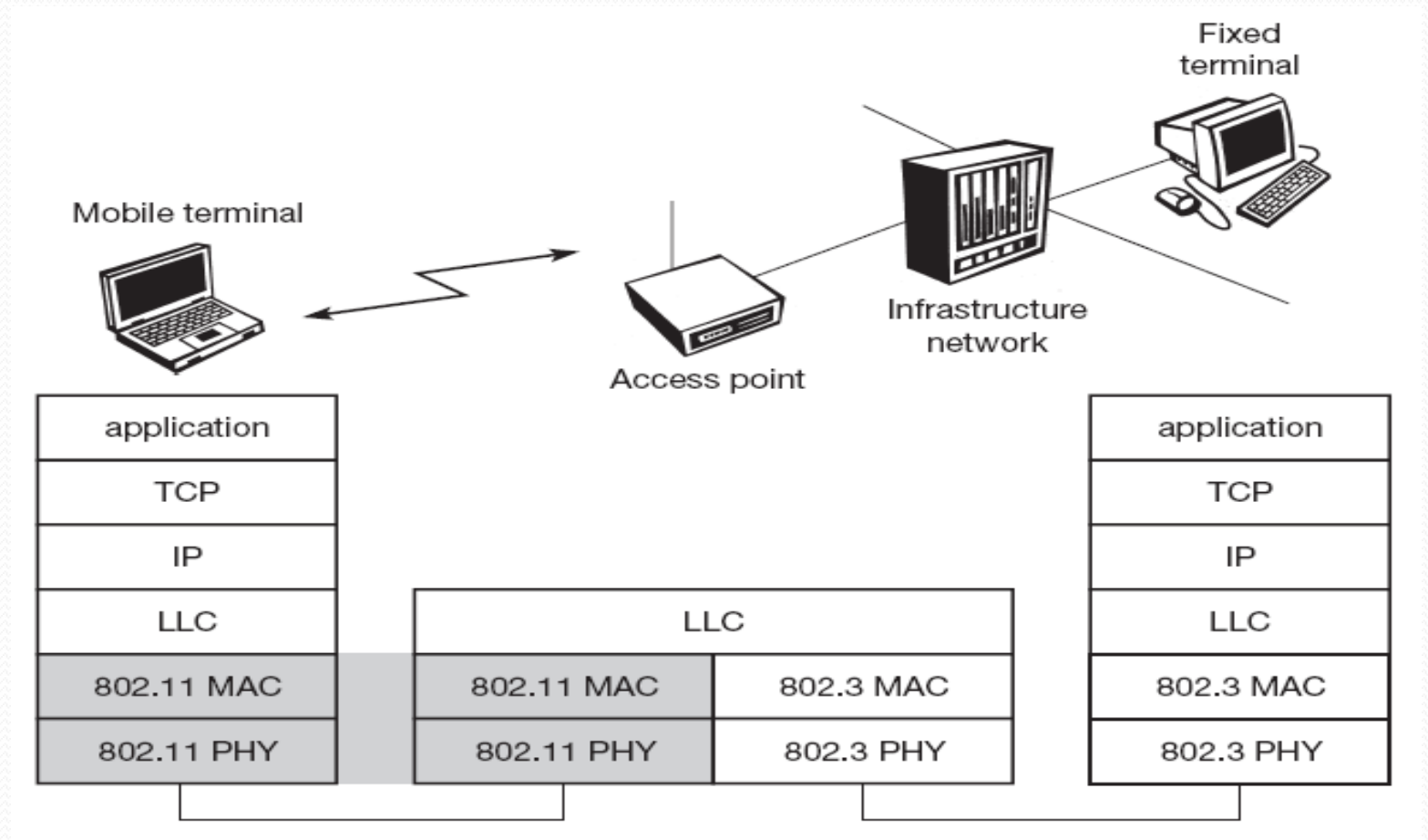
IEEE 802.11: System architecture

- IEEE 802.11 allows the building of **ad-hoc networks** between stations, forming one or more **independent BSSs** (IBSS)
- An **IBSS** comprises a group of stations using **the same radio frequency**.
- IEEE 802.11 does not specify **any special nodes** that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN1 or bluetooth.



Protocol architecture

- The higher layers (application, TCP, IP) look the same for wireless nodes as for wired nodes.
- The upper part of the **DLC (data link control) layer**, the **logical link control (LLC)**, covers the differences of the medium access control layers needed for the different media



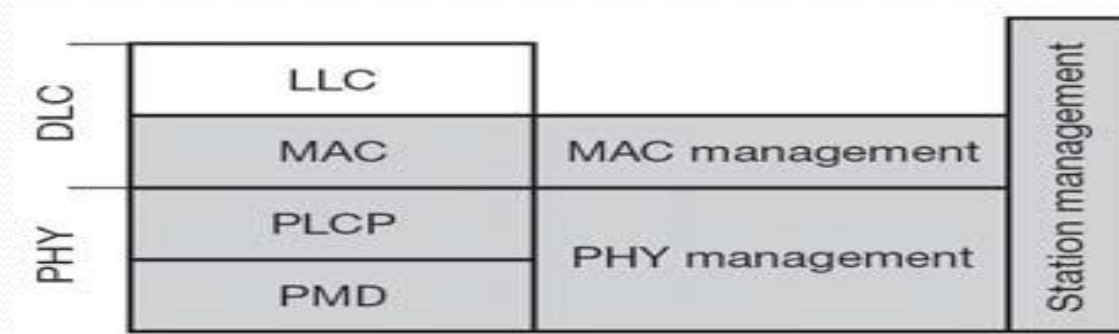
IEEE 802.11: System architecture

- The physical layer is subdivided into:
 - the Physical Layer Convergence Protocol (PLCP)
 - It provides a carrier sense signal, called Clear Channel Assessment (CCA)
 - It provides a common PHY Service Access Point (SAP) independent of the transmission technology.
 - the Physical Medium Dependent sublayer PMD
 - It handles modulation and encoding/decoding of signals.
- The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.

IEEE 802.11: System architecture

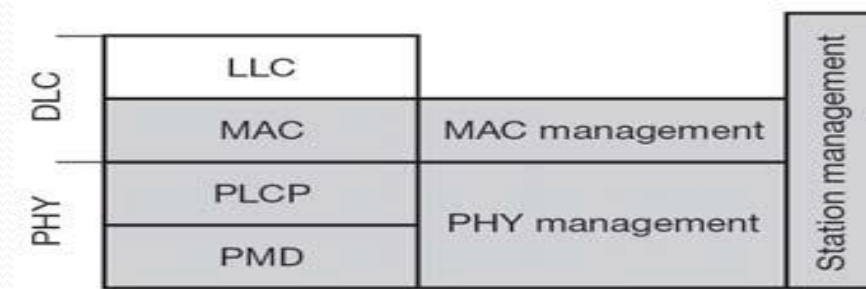
□ The MAC management:

- supports the **association** & **re-association** of a station to an AP and **roaming** between different APs.
- controls **authentication** mechanisms, **encryption**, **synchronization** of a station with regard to an AP , and power management to save battery power.
- maintains the MAC **management information base** (MIB).



IEEE 802.11: System architecture

- The PHY management :
 - include channel tuning and PHY MIB maintenance.
- Station management
 - interacts with both management layers
 - is responsible for additional higher layer functions (e.g., control of bridging and interaction with the DS in the case of an AP).



IEEE 802.11 family

- The **initial** standard gives a maximum data rate of **2 Mbps...**
- The **next** standard, **IEEE 802.11b** , increases the rate to 11 Mbps.
- With the introduction of newer standards, **IEEE 802.11a** and **IEEE 802.11g** , the data rate increases to **54 Mbps**.
- Additional mechanisms have been developed to remedy QoS support **IEEE 802.11e** and security problems **IEEE 802.11i**.

IEEE 802.11 family

- **IEEE 802.11n**, standardizes these efforts and introduce new **MAC enhancements** to overcome MAC layer limitations in the previous
 - It supports very high data rates up to 600 Mbps and use the QoS mechanisms introduced by IEEE 802.11e.
- **802.11s**, which adds mesh topology support to the IEEE 802.11.
 - Chipset vendors that develop WLAN devices based on IEEE 802.11 standard have formed a consortium called **WiFi alliance for interoperability** between devices from different companies.
 - **WiFi also supports devices using HiperLAN standard.**
 - Currently, the terms IEEE 802.11 and WiFi are used interchangeably in the literature.

IEEE 802.11 family

Standard	Year Released	Frequency (GHz)	Speed
802.11	1997	2.4	2 Mbps
802.11a	1999	5	1.5-54 Mbps
802.11b	1999	2.4	11 Mbps
802.11g	2003	2.4	54 Mbps
802.11n	2009	2.4/5	Up to 600 Mbps
802.11ac	2013	5	Up to 3.5 Gbps
802.11ax	2019	2.4/5	Up to 9.6 Gbps
802.11be	2024	2.4/5/6	Up to 46 Gbps

IEEE 802.11 family

□ Key 802.11 standards and their applications:

- **802.11a:** An early Wi-Fi standard suitable for basic wireless networking and light data tasks in small areas, though it's largely obsolete in modern networks.
- **802.11b/g/n:** Suitable for general home and small business use due to decent range and good compatibility with older devices.
- **802.11ac:** Ideal for most home networks and small businesses, 802.11ac provides sufficient speed and performance for everyday internet use, and office work.
- **802.11ax:** Offers better performance, efficiency, and capacity, well-suited for dense environments like stadiums, airports, and large enterprise deployments.
- **802.11be:** Delivers greater capacity and lower latency, making it perfect for immersive AR/VR experiences, high-quality video conferencing, real-time collaboration, cloud computing, industrial IoT, and highly interactive telemedicine applications

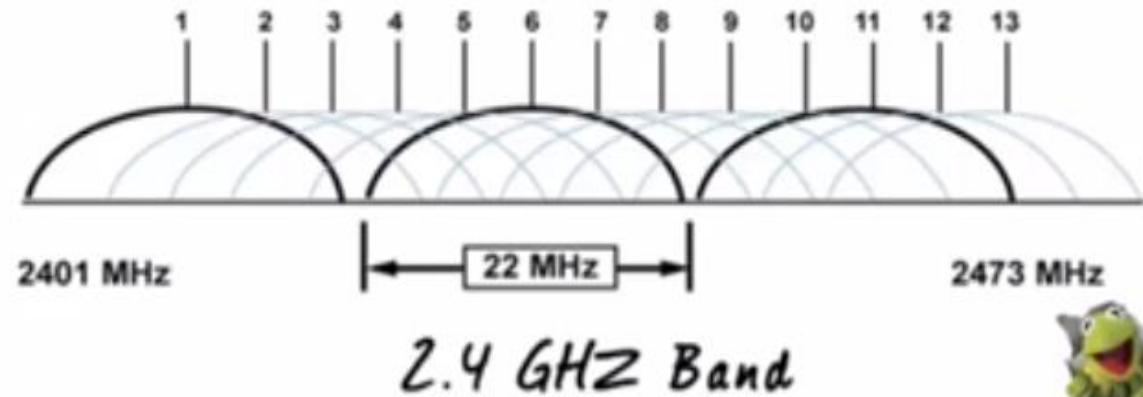
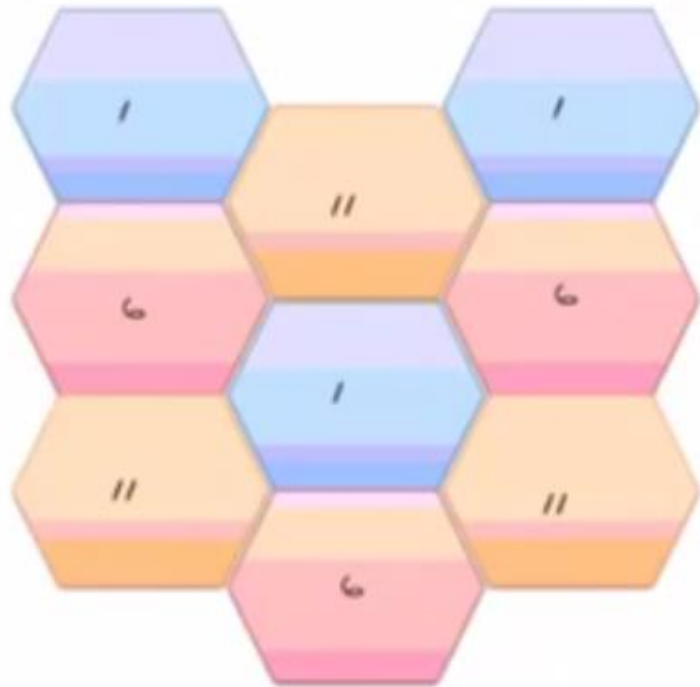
Physical (PHY) layer

Channel	Frequency [MHz]	US/Canada	Europe	Japan
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467	—	X	X
13	2472	—	X	X
14	2484	—	—	X

Physical (PHY) layer

- IEEE 802.11 , **rule**: the center frequency of channels must be at least **5 MHz apart** from each other and the power levels of the signals for nearby frequencies cannot exceed **certain thresholds**.
- A typical APs signal does not extend more than 22 MHz from center frequency of the selected frequency.
 - the channel bandwidth of IEEE 802.11 is in effect 22 MHz.
- As a result only three of the 14 channels do not overlap.

Physical (PHY) layer





Thank you,
Questions???